Spawning shells

Non-interactive tty-shell

If you have a non-tty-shell there are certain commands and stuff you can't do. This can happen if you upload reverse shells on a webserver, so that the shell you get is by the user www-data, or similar. These users are not meant to have shells as they don't interact with the system has humans do.

So if you don't have a tty-shell you can't run `su`, `sudo` for example. This can be annoying if you manage to get a root password but you can't use it.

Anyways, if you get one of these shells you can upgrade it to a tty-shell using the following methods:

Using python

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

Echo

```
echo 'os.system('/bin/bash')'
```

sh

```
/bin/sh -i
```

bash

```
/bin/bash -i
```

Perl

```
perl -e 'exec "/bin/sh";'
```

From within VI

```
:!bash
```

Interactive tty-shell

So if you manage to upgrade to a non-interactive tty-shell you will still have a limited shell. You won't be able to use the up and down arrows, you won't have tab-completion. This might be really frustrating if you stay in that shell for long. It can also be more risky, if a execution gets stuck you cant use Ctr-C or Ctr-Z without killing your session. However that can be fixed using socat. Follow these instructions.

https://github.com/cornerpirate/socat-shell

References:

http://unix.stackexchange.com/questions/122616/why-do-i-need-a-tty-to-run-sudo-if-i-can-sudo-without-a-password http://netsec.ws/?p=337
http://pentestmonkey.net/blog/post-exploitation-without-a-tty